

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours
NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.		
RESPONSE DUE: Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met. Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met. By the later of 24 hours after the recognition of the incident <u>OR</u> by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. <i>Nota 4 00pm local time will be considered the end of the business day</i> Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident. For NERC reporting entities registered in the United States; NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.		
<p style="text-align: center;">METHODS OF FILING RESPONSE (Retain a completed copy of this form for your files.)</p> <p>Online: Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/ FAX: FAX Form OE-417 to the following facsimile number: (202) 586-8485. Alternate: If you are unable to submit online or by fax, forms may be e-mailed to doehqec@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.</p>		
<p style="text-align: center;">SCHEDULE 1 -- ALERT CRITERIA (Page 1 of 4)</p>		
<p style="text-align: center;">Criteria for Filing (Check all that apply) See Instructions For More Information</p>		
<p>EMERGENCY ALERT File within 1-Hour</p> <p>If any box 1-8 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on Line A below.</p>	<ol style="list-style-type: none"> 1. <input type="checkbox"/> Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. <input checked="" type="checkbox"/> Cyber event that causes interruptions of electrical system operations 3. <input type="checkbox"/> Complete operational failure or shut-down of the transmission and/or distribution electrical system 4. <input type="checkbox"/> Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system 5. <input type="checkbox"/> Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident 6. <input type="checkbox"/> Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 7. <input type="checkbox"/> System-wide voltage reductions of 3 percent or more 8. <input type="checkbox"/> Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System 	
<p>NORMAL REPORT File within 6-Hours</p> <p>If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on Line A below.</p>	<ol style="list-style-type: none"> 9. <input type="checkbox"/> Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems 10. <input checked="" type="checkbox"/> Cyber event that could potentially impact electric power system adequacy or reliability 11. <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more 12. <input type="checkbox"/> Fuel supply emergencies that could impact electric power system adequacy or reliability 	

SCHEDULE 1 -- ALERT CRITERIA -- CONTINUED

(Page 2 of 4)

SYSTEM REPORT

File within 1-Business Day

If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident OR by the end of the next business day. *Note* 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert Status) on Line A below.

13. ☐ Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a Bulk Electric System Emergency.
14. ☐ Damage or destruction of its Facility that results from actual or suspected intentional human action.
15. ☐ Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.
16. ☐ Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.
17. ☐ Bulk Electric System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.
18. ☐ Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts
19. ☐ Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.
20. ☐ Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.
21. ☐ Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).
22. ☐ Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.
23. ☐ Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more.
24. ☐ Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.

If significant changes have occurred after filing the initial report, re-file the form with the changes and check Update (for the Alert Status) on Line A below.

The form must be re-filed within 72 hours of the incident with the latest information and Final (Alert Status) checked on Line A below, unless updated.

LINE NO.						
A.	Alert Status (check one)	Emergency Alert <input checked="" type="checkbox"/> 1 Hour	Normal Report <input type="checkbox"/> 6 Hours	System Report <input type="checkbox"/> 1 Business Day	Update <input type="checkbox"/> As required	Final <input type="checkbox"/> 72 Hours
B.	Organization Name	sPower				
C.	Address of Principal Business Office	2180 South 1300 East Suite 600 Salt Lake City Utah 84106				

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417		ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT		OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours	
SCHEDULE 1 -- ALERT NOTICE					
(Page 3 of 4)					
INCIDENT AND DISTURBANCE DATA					
D.	Geographic Area(s) Affected (County, State)	California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County;			
E.	Date/Time Incident Began (mm-dd-yy/hh:mm) using 24-hour clock	03 - 05 - 2019 / 09 : 12 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	03 - 05 - 2019 / 18 : 57 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Unknown <input checked="" type="checkbox"/>	
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	
I.	Estimate of Number of Customers Affected		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	

SCHEDULE 1 - TYPE OF EMERGENCY		
Check all that apply		
J. Cause	K. Impact	L. Action Taken
<input type="checkbox"/> Unknown <input type="checkbox"/> Physical attack <input type="checkbox"/> Threat of physical attack <input type="checkbox"/> Vandalism <input type="checkbox"/> Theft <input type="checkbox"/> Suspicious activity <input type="checkbox"/> Cyber event (information technology) <input checked="" type="checkbox"/> Cyber event (operational technology) <input type="checkbox"/> Fuel supply emergencies, interruption, or deficiency <input type="checkbox"/> Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure <input type="checkbox"/> Transmission equipment failure (not including substation or switchyard) <input type="checkbox"/> Failure at high voltage substation or switchyard <input type="checkbox"/> Weather or natural disaster <input type="checkbox"/> Operator action(s) <input type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Initial assessment revealed that a firewall exploit was likely utilized to execute a denial of service attack that caused the firewalls to reboot leading to an approximately 5 minute communications outage	<input type="checkbox"/> None <input type="checkbox"/> Control center loss, failure, or evacuation <input type="checkbox"/> Loss or degradation of control center monitoring or communication systems <input type="checkbox"/> Damage or destruction of a facility <input type="checkbox"/> Electrical system separation (islanding) <input type="checkbox"/> Complete operational failure or shutdown of the transmission and/or distribution system <input type="checkbox"/> Major transmission system interruption (three or more BES elements) <input type="checkbox"/> Major distribution system interruption <input type="checkbox"/> Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more <input type="checkbox"/> System-wide voltage reductions or 3 percent or more <input type="checkbox"/> Voltage deviation on an individual facility of ≥10% for 15 minutes or more <input type="checkbox"/> Inadequate electric resources to serve load <input type="checkbox"/> Generating capacity loss of 1,400 MW or more <input type="checkbox"/> Generating capacity loss of 2,000 MW or more <input type="checkbox"/> Complete loss of off-site power to a nuclear generating station <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximately 5 minutes) between field devices at sites and between the sites and sPower's Control Center	<input type="checkbox"/> None <input type="checkbox"/> Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) <input type="checkbox"/> Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system <input type="checkbox"/> Implemented a warning, alert, or contingency plan <input type="checkbox"/> Voltage reduction <input type="checkbox"/> Shed Interruptible Load <input type="checkbox"/> Repaired or restored <input type="checkbox"/> Mitigation implemented <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: After learning of the potential cause of the reboot, sPower started testing and deployment of an update to remove the exploited vulnerability

U.S. Department of Energy
Electricity Delivery and
Energy Reliability
Form OE-417

**ELECTRIC EMERGENCY INCIDENT AND
DISTURBANCE REPORT**

OMB No. 1901-0288
Approval Expires: 05/31/2021
Burden Per Response: 1.8 hours

SCHEDULE 2 – NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION

M.	Name	Lucas Root
N.	Title	Director, Operations
O.	Telephone Number	(801)-(679)-(3527)
P.	FAX Number	() () ()
Q.	E-mail Address	lroot@spower.com

Provide a description of the incident and actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Be sure to identify: the estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can be supplied to meet the requirement; this includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 needs to be filed. Check the Final box on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours after detection that a criterion was met.

R. Narrative:

This information will be provided in a subsequent update after additional information gathering

**S. Estimated Restoration Date for all Affected Customers
Who Can Receive Power**

mo dd yy

T. Name of Assets Impacted

Pioneer, Beacon 4, ABSR, DSR1, DSR2, Beacon 1, Elevation C, WABSRB, Bayshore A, Bayshore B, Bayshore C, and Solverde.

U. Notify NERC/E-ISAC

Select if you approve of all of the information provided on the Form being submitted to the North America Electric Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-ISAC).

NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards.

If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC.

☒ Notify NERC | ☒ Notify E-ISAC

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours
NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.		
RESPONSE DUE: Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met. Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met. By the later of 24 hours after the recognition of the incident <u>OR</u> by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. <i>Note: 4:00pm local time will be considered the end of the business day.</i> Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident. For NERC reporting entities registered in the United States, NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.		
<p style="text-align: center;">METHODS OF FILING RESPONSE (Retain a completed copy of this form for your files.)</p> <p>Online: Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/ FAX: FAX Form OE-417 to the following facsimile number: (202) 586-8485. Alternate: If you are unable to submit online or by fax, forms may be e-mailed to doehqroc@hq.doe.gov, or call and report the information to the following telephone number: (202) 586-8100.</p>		

SCHEDULE 1 -- ALERT CRITERIA

(Page 1 of 4)

Criteria for Filing (Check all that apply)
See Instructions For More Information

<p style="text-align: center;">EMERGENCY ALERT File within 1-Hour</p> <p>If any box 1-8 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on Line A below.</p>	<p>1. <input type="checkbox"/> Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations</p> <p>2. <input checked="" type="checkbox"/> Cyber event that causes interruptions of electrical system operations</p> <p>3. <input type="checkbox"/> Complete operational failure or shut-down of the transmission and/or distribution electrical system</p> <p>4. <input type="checkbox"/> Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system</p> <p>5. <input type="checkbox"/> Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident</p> <p>6. <input type="checkbox"/> Firm load shedding of 100 Megawatts or more implemented under emergency operational policy</p> <p>7. <input type="checkbox"/> System-wide voltage reductions of 3 percent or more</p> <p>8. <input type="checkbox"/> Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System</p>
<p style="text-align: center;">NORMAL REPORT File within 6-Hours</p> <p>If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on Line A below.</p>	<p>9. <input type="checkbox"/> Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems</p> <p>10. <input checked="" type="checkbox"/> Cyber event that could potentially impact electric power system adequacy or reliability</p> <p>11. <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more</p> <p>12. <input type="checkbox"/> Fuel supply emergencies that could impact electric power system adequacy or reliability</p>

SCHEDULE 1 -- ALERT CRITERIA -- CONTINUED

(Page 2 of 4)

<p>SYSTEM REPORT File within 1-Business Day</p> <p>If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident <u>OR</u> by the end of the next business day. <i>Note</i> 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert Status) on Line A below.</p>	<p>13. <input type="checkbox"/> Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a Bulk Electric System Emergency.</p> <p>14. <input type="checkbox"/> Damage or destruction of its Facility that results from actual or suspected intentional human action.</p> <p>15. <input type="checkbox"/> Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.</p> <p>16. <input type="checkbox"/> Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.</p> <p>17. <input type="checkbox"/> Bulk Electric System Emergency resulting in voltage deviation on a Facility; A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.</p> <p>18. <input type="checkbox"/> Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts</p> <p>19. <input type="checkbox"/> Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.</p> <p>20. <input type="checkbox"/> Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.</p> <p>21. <input type="checkbox"/> Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).</p> <p>22. <input type="checkbox"/> Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.</p> <p>23. <input type="checkbox"/> Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more.</p> <p>24. <input type="checkbox"/> Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.</p>
--	---

If significant changes have occurred after filing the initial report, re-file the form with the changes and check Update (for the Alert Status) on Line A below.

The form must be re-filed within 72 hours of the incident with the latest information and Final (Alert Status) checked on Line A below, unless updated

LINE NO.						
A.	Alert Status (check one)	Emergency Alert <input type="checkbox"/> 1 Hour	Normal Report <input type="checkbox"/> 6 Hours	System Report <input type="checkbox"/> 1 Business Day	Update <input checked="" type="checkbox"/> As required	Final <input type="checkbox"/> 72 Hours
B.	Organization Name	sPower				
C.	Address of Principal Business Office	2180 South 1300 East Suite 600 Salt Lake City Utah 84106				

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417		ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT		OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours	
SCHEDULE 1 -- ALERT NOTICE (Page 3 of 4)					
INCIDENT AND DISTURBANCE DATA					
D.	Geographic Area(s) Affected (County, State)	California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County;			
E.	Date/Time Incident Began (mm-dd-yy/hh:mm) using 24-hour clock	03 - 05 - 2019 / 09 : 12 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	03 - 05 - 2019 / 18 : 57 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Unknown <input checked="" type="checkbox"/>	
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	
I.	Estimate of Number of Customers Affected		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	

SCHEDULE 1 -- TYPE OF EMERGENCY Check all that apply		
J. Cause	K. Impact	L. Action Taken
<input type="checkbox"/> Unknown <input type="checkbox"/> Physical attack <input type="checkbox"/> Threat of physical attack <input type="checkbox"/> Vandalism <input type="checkbox"/> Theft <input type="checkbox"/> Suspicious activity <input type="checkbox"/> Cyber event (information technology) <input checked="" type="checkbox"/> Cyber event (operational technology) <input type="checkbox"/> Fuel supply emergencies, interruption, or deficiency <input type="checkbox"/> Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure <input type="checkbox"/> Transmission equipment failure (not including substation or switchyard) <input type="checkbox"/> Failure at high voltage substation or switchyard <input type="checkbox"/> Weather or natural disaster <input type="checkbox"/> Operator action(s) <input type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Initial assessment revealed that a firewall exploit was likely utilized to execute a denial of service attack that caused the firewalls to reboot leading to an approximately 5 minute communications outage	<input type="checkbox"/> None <input type="checkbox"/> Control center loss, failure, or evacuation <input type="checkbox"/> Loss or degradation of control center monitoring or communication systems <input type="checkbox"/> Damage or destruction of a facility <input type="checkbox"/> Electrical system separation (islanding) <input type="checkbox"/> Complete operational failure or shutdown of the transmission and/or distribution system <input type="checkbox"/> Major transmission system interruption (three or more BES elements) <input type="checkbox"/> Major distribution system interruption <input type="checkbox"/> Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more <input type="checkbox"/> System-wide voltage reductions or 3 percent or more <input type="checkbox"/> Voltage deviation on an individual facility of ≥10% for 15 minutes or more <input type="checkbox"/> Inadequate electric resources to serve load <input type="checkbox"/> Generating capacity loss of 1,400 MW or more <input type="checkbox"/> Generating capacity loss of 2,000 MW or more <input type="checkbox"/> Complete loss of off-site power to a nuclear generating station <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximately 5 minutes) between field devices at sites and between the sites and sPower's Control Center	<input type="checkbox"/> None <input type="checkbox"/> Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) <input type="checkbox"/> Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system <input type="checkbox"/> Implemented a warning, alert, or contingency plan <input type="checkbox"/> Voltage reduction <input type="checkbox"/> Shed Interruptible Load <input type="checkbox"/> Repaired or restored <input type="checkbox"/> Mitigation implemented <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: After learning of the potential cause of the reboot, sPower started testing and deployment of an update to remove the exploited vulnerability

U.S. Department of Energy
Electricity Delivery and
Energy Reliability
Form OE-417

**ELECTRIC EMERGENCY INCIDENT AND
DISTURBANCE REPORT**

OMB No. 1901-0288
Approval Expires: 05/31/2021
Burden Per Response: 1.8 hours

SCHEDULE 2 -- NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION

M.	Name	Lucas Root
N.	Title	Director, Operations
O.	Telephone Number	(801)-(679)-(3527)
P.	FAX Number	() () ()
Q.	E-mail Address	lroot@spower.com

Provide a description of the incident and actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Be sure to identify: the estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can be supplied to meet the requirement; this includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 needs to be filed. Check the Final box on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours after detection that a criterion was met.

R. Narrative:

sPower is a Generator Owner and Generator Operator of wind and solar generation assets that are operated from a Control Center in Salt Lake City, UT. (b) (7)(E)

These updates are ongoing.

**S. Estimated Restoration Date for all Affected Customers
Who Can Receive Power**

mo dd yy

T. Name of Assets Impacted

Pioneer, Beacon 4, ABSR, DSR1, DSR2, Beacon 1, Elevation C, WABSRB, Bayshore A, Bayshore B, Bayshore C, Solverde, firewall at sPower headquarters

U. Notify NERC/E-ISAC

Select if you approve of all of the information provided on the Form being submitted to the North America Electric Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-ISAC).

NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards.

If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC.

☒ Notify NERC | ☒ Notify E-ISAC

Document 3

From: Tarduogno, Matthew
To: Evans, Karen S; Lotto, Adrienne
Cc: Kenneth Buell (Kenneth.Buell@hq.doe.gov); Kumar, Presh
Subject: Follow-Up on Denial of Service Incident
Date: Friday, March 08, 2019 5:59:00 PM

OFFICIAL USE ONLY

All,

I wanted to quickly follow-up on the denial-of-service (DoS) incident experienced by sPower, a company that owns and operators solar and wind generation assets in several states, that we noted this morning. I spoke with the operations manager of sPower this morning and the E-ISAC has also been in contact with the company.

On March 5, sPower noted a series of brief communication outages between their control center and their remote sites. Upon further investigation, the communications outages were determined to have been caused by firewall reboots. After consulting with Cisco, the firewall manufacture, it was determined that the firewall reboots were caused by a DoS attack exploiting a known vulnerability. Cisco recommended a firmware update, which sPower has been deploying across their system, after testing for compatibility. The DoS incident was observed intermittently over a 12 hour period and no further activity has been observed since this time. sPower has reviewed log files and has found no evidence of a breach beyond the DoS attack. Additionally, the incident did not have any impacts on operations.

When I spoke with sPower they did not expect to need any additional support or have any ongoing concerns; however, they will contact us if there are any issues. (b) (7)(E)

We have been providing DOE's Office of Intelligence and Counterintelligence with updates and they are ready to investigate any indicators, as appropriate, and have been checking for any related incidents. We will work with IN and the ISACs to provide appropriate information to the sector as available.

Please let me know if you have any questions.

Best Regards,

-Matt

Matthew T. Tarduogno

Infrastructure Security & Energy Restoration

Office of Cybersecurity, Energy Security, & Emergency Response

U.S. Department of Energy

Office: 202-586-2892 | Mobile: (b) (6)

Matthew.Tarduogno@hq.doe.gov

OFFICIAL USE ONLY

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417	<i>ELECTRIC EMERGENCY INCIDENT AND</i> <i>DISTURBANCE REPORT</i>	OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours
NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.		
RESPONSE DUE: Within 1 hour of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as an Emergency Alert report if criteria 1-8 are met. Within 6 hours of the incident, submit Schedule 1 and lines M - Q in Schedule 2 as a Normal Report if only criteria 9-12 are met. By the later of 24 hours after the recognition of the incident OR by the end of the next business day submit Schedule 1 & lines M - Q in Schedule 2 as a System Report if criteria 13-24 are met. <i>Note: 4:00pm local time will be considered the end of the business day.</i> Submit updates as needed and/or a final report (all of Schedules 1 and 2) within 72 hours of the incident. For NERC reporting entities registered in the United States, NERC has approved that the form OE-417 meets the submittal requirements for NERC. There may be other applicable regional, state and local reporting requirements.		
METHODS OF FILING RESPONSE (Retain a completed copy of this form for your files.)		
Online: Submit form via online submission at: https://www.oe.netl.doe.gov/OE417/ FAX: FAX Form OE-417 to the following facsimile number: (202) 586-8485. Alternate: If you are unable to submit online or by fax, forms may be e-mailed to doehqoc@hq.doe.gov , or call and report the information to the following telephone number: (202) 586-8100.		
SCHEDULE 1 -- ALERT CRITERIA (Page 1 of 4)		
Criteria for Filing (Check all that apply) See Instructions For More Information		
EMERGENCY ALERT File within 1-Hour If any box 1-8 on the right is checked, this form must be filed within 1 hour of the incident; check Emergency Alert (for the Alert Status) on Line A below.	1. <input type="checkbox"/> Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations 2. <input checked="" type="checkbox"/> Cyber event that causes interruptions of electrical system operations 3. <input type="checkbox"/> Complete operational failure or shut-down of the transmission and/or distribution electrical system 4. <input type="checkbox"/> Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system 5. <input type="checkbox"/> Uncontrolled loss of 300 Megawatts or more of firm system loads for 15 minutes or more from a single incident 6. <input type="checkbox"/> Firm load shedding of 100 Megawatts or more implemented under emergency operational policy 7. <input type="checkbox"/> System-wide voltage reductions of 3 percent or more 8. <input type="checkbox"/> Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the Bulk Electric System	
NORMAL REPORT File within 6-Hours If any box 9-12 on the right is checked AND none of the boxes 1-8 are checked, this form must be filed within 6 hours of the incident; check Normal Report (for the Alert Status) on Line A below.	9. <input type="checkbox"/> Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems 10. <input checked="" type="checkbox"/> Cyber event that could potentially impact electric power system adequacy or reliability 11. <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more 12. <input type="checkbox"/> Fuel supply emergencies that could impact electric power system adequacy or reliability	

SCHEDULE 1 -- ALERT CRITERIA -- CONTINUED

(Page 2 of 4)

<p>SYSTEM REPORT File within 1-Business Day</p> <p>If any box 13-24 on the right is checked AND none of the boxes 1-12 are checked, this form must be filed by the later of 24 hours after the recognition of the incident OR by the end of the next business day. <i>Note</i> 4:00pm local time will be considered the end of the business day. Check System Report (for the Alert Status) on Line A below.</p>	<p>13. <input type="checkbox"/> Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in action(s) to avoid a Bulk Electric System Emergency.</p> <p>14. <input type="checkbox"/> Damage or destruction of its Facility that results from actual or suspected intentional human action.</p> <p>15. <input type="checkbox"/> Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. Or suspicious device or activity at its Facility.</p> <p>16. <input type="checkbox"/> Physical threat to its Bulk Electric System control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. Or suspicious device or activity at its Bulk Electric System control center.</p> <p>17. <input type="checkbox"/> Bulk Electric System Emergency resulting in voltage deviation on a Facility. A voltage deviation equal to or greater than 10% of nominal voltage sustained for greater than or equal to 15 continuous minutes.</p> <p>18. <input type="checkbox"/> Uncontrolled loss of 200 Megawatts or more of firm system loads for 15 minutes or more from a single incident for entities with previous year's peak demand less than or equal to 3,000 Megawatts</p> <p>19. <input type="checkbox"/> Total generation loss, within one minute of: greater than or equal to 2,000 Megawatts in the Eastern or Western Interconnection or greater than or equal to 1,400 Megawatts in the ERCOT Interconnection.</p> <p>20. <input type="checkbox"/> Complete loss of off-site power (LOOP) affecting a nuclear generating station per the Nuclear Plant Interface Requirements.</p> <p>21. <input type="checkbox"/> Unexpected Transmission loss within its area, contrary to design, of three or more Bulk Electric System Facilities caused by a common disturbance (excluding successful automatic reclosing).</p> <p>22. <input type="checkbox"/> Unplanned evacuation from its Bulk Electric System control center facility for 30 continuous minutes or more.</p> <p>23. <input type="checkbox"/> Complete loss of Interpersonal Communication and Alternative Interpersonal Communication capability affecting its staffed Bulk Electric System control center for 30 continuous minutes or more.</p> <p>24. <input type="checkbox"/> Complete loss of monitoring or control capability at its staffed Bulk Electric System control center for 30 continuous minutes or more.</p>
---	---

If significant changes have occurred after filing the initial report, re-file the form with the changes and check Update (for the Alert Status) on Line A below.

The form must be re-filed within 72 hours of the incident with the latest information and Final (Alert Status) checked on Line A below, unless updated

LINE NO.						
A.	Alert Status (check one)	Emergency Alert <input type="checkbox"/> 1 Hour	Normal Report <input type="checkbox"/> 6 Hours	System Report <input type="checkbox"/> 1 Business Day	Update <input type="checkbox"/> As required	Final <input checked="" type="checkbox"/> 72 Hours
B.	Organization Name	sPower				
C.	Address of Principal Business Office	2180 South 1300 East Suite 600 Salt Lake City Utah 84106				

U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417		ELECTRIC EMERGENCY INCIDENT AND DISTURBANCE REPORT		OMB No. 1901-0288 Approval Expires: 05/31/2021 Burden Per Response: 1.8 hours	
SCHEDULE 1 -- ALERT NOTICE (Page 3 of 4)					
INCIDENT AND DISTURBANCE DATA					
D.	Geographic Area(s) Affected (County, State)	California: Kern County, Los Angeles County; Utah: Salt Lake County; Wyoming: Converse County;			
E.	Date/Time Incident Began (mm-dd-yy/hh:mm) using 24-hour clock	03 - 05 - 2019 / 09 : 12 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
F.	Date/Time Incident Ended (mm-dd-yy/ hh:mm) using 24-hour clock	03 - 05 - 2019 / 18 : 57 mo dd yy hh mm	<input type="checkbox"/> Eastern <input type="checkbox"/> Pacific	<input type="checkbox"/> Central <input type="checkbox"/> Alaska	<input checked="" type="checkbox"/> Mountain <input type="checkbox"/> Hawaii
G.	Did the incident/disturbance originate in your system/area? (check one)	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Unknown <input checked="" type="checkbox"/>	
H.	Estimate of Amount of Demand Involved (Peak Megawatts)		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	
I.	Estimate of Number of Customers Affected		Zero <input checked="" type="checkbox"/>	Unknown <input type="checkbox"/>	

SCHEDULE 1 -- TYPE OF EMERGENCY

Check all that apply

J. Cause	K. Impact	L. Action Taken
<input type="checkbox"/> Unknown <input type="checkbox"/> Physical attack <input type="checkbox"/> Threat of physical attack <input type="checkbox"/> Vandalism <input type="checkbox"/> Theft <input type="checkbox"/> Suspicious activity <input type="checkbox"/> Cyber event (information technology) <input checked="" type="checkbox"/> Cyber event (operational technology) <input type="checkbox"/> Fuel supply emergencies, interruption, or deficiency <input type="checkbox"/> Generator loss or failure not due to fuel supply interruption or deficiency or transmission failure <input type="checkbox"/> Transmission equipment failure (not including substation or switchyard) <input type="checkbox"/> Failure at high voltage substation or switchyard <input type="checkbox"/> Weather or natural disaster <input type="checkbox"/> Operator action(s) <input type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Initial assessment revealed that a firewall exploit was likely utilized to execute a denial of service attack that caused the firewalls to reboot leading to an approximately 5 minute or less communications outage	<input type="checkbox"/> None <input type="checkbox"/> Control center loss, failure, or evacuation <input type="checkbox"/> Loss or degradation of control center monitoring or communication systems <input type="checkbox"/> Damage or destruction of a facility <input type="checkbox"/> Electrical system separation (islanding) <input type="checkbox"/> Complete operational failure or shutdown of the transmission and/or distribution system <input type="checkbox"/> Major transmission system interruption (three or more BES elements) <input type="checkbox"/> Major distribution system interruption <input type="checkbox"/> Uncontrolled loss of 200 MW or more of firm system loads for 15 minutes or more <input type="checkbox"/> Loss of electric service to more than 50,000 customers for 1 hour or more <input type="checkbox"/> System-wide voltage reductions or 3 percent or more <input type="checkbox"/> Voltage deviation on an individual facility of ≥10% for 15 minutes or more <input type="checkbox"/> Inadequate electric resources to serve load <input type="checkbox"/> Generating capacity loss of 1,400 MW or more <input type="checkbox"/> Generating capacity loss of 2,000 MW or more <input type="checkbox"/> Complete loss of off-site power to a nuclear generating station <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: Firewall reboots resulted in brief communications outages (approximately 5 minutes or less) between field devices at sites and between the sites and sPower's Control Center	<input type="checkbox"/> None <input type="checkbox"/> Shed Firm Load: Load shedding of 100 MW or more implemented under emergency operational policy (manually or automatically via UFLS or remedial action scheme) <input type="checkbox"/> Public appeal to reduce the use of electricity for the purpose of maintaining the continuity of the electric power system <input type="checkbox"/> Implemented a warning, alert, or contingency plan <input type="checkbox"/> Voltage reduction <input type="checkbox"/> Shed Interruptible Load <input type="checkbox"/> Repaired or restored <input type="checkbox"/> Mitigation implemented <input checked="" type="checkbox"/> Other <input checked="" type="checkbox"/> Additional Information/Comments: After learning of the potential cause of the reboot, sPower started testing and deployment of an update to remove the exploited vulnerability

U.S. Department of Energy
Electricity Delivery and
Energy Reliability
Form OE-417

**ELECTRIC EMERGENCY INCIDENT AND
DISTURBANCE REPORT**

OMB No. 1901-0288
Approval Expires: 05/31/2021
Burden Per Response: 1.8 hours

SCHEDULE 2 – NARRATIVE DESCRIPTION

(Page 4 of 4)

Information on Schedule 2 will not be disclosed to the public to the extent that it satisfies the criteria for exemption under the Freedom of Information Act, e.g., exemptions for confidential commercial information and trade secrets, certain information that could endanger the physical safety of an individual, or information designated as Critical Energy Infrastructure Information.

NAME OF OFFICIAL THAT SHOULD BE CONTACTED FOR FOLLOW-UP OR ANY ADDITIONAL INFORMATION

M.	Name	Lucas Root
N.	Title	Director, Operations
O.	Telephone Number	(801)-(679)-3527
P.	FAX Number	() () ()
Q.	E-mail Address	lroot@spower.com

Provide a description of the incident and actions taken to resolve it. Include as appropriate, the cause of the incident/disturbance, change in frequency, mitigation actions taken, equipment damaged, critical infrastructures interrupted, effects on other systems, and preliminary results from any investigations. Be sure to identify: the estimate restoration date, the name of any lost high voltage substations or switchyards, whether there was any electrical system separation (and if there were, what the islanding boundaries were), and the name of the generators and voltage lines that were lost (shown by capacity type and voltage size grouping). If necessary, copy and attach additional sheets. Equivalent documents, containing this information can be supplied to meet the requirement; this includes the NERC EOP-004 Disturbance Report. Along with the filing of Schedule 2, a final (updated) Schedule 1 needs to be filed. Check the Final box on line A for Alert Status on Schedule 1 and submit this and the completed Schedule 2 no later than 72 hours after the incident that a critical facility was lost.

R. Narrative:

sPower is a Generator Owner and Generator Operator of wind and solar generation assets that are operated from a Control Center in Salt Lake City, UT. (b) (7)(E)

**S. Estimated Restoration Date for all Affected Customers
Who Can Receive Power**

mo dd yy

T. Name of Assets Impacted

Pioneer, Beacon 4, ABSR, DSR1, DSR2, Beacon 1, Elevation C, WAASRB, Bayshore A, Bayshore B, Bayshore C, Solverde, firewall at sPower headquarters

U. Notify NERC/E-ISAC

Select if you approve of all of the information provided on the Form being submitted to the North America Electric Reliability Corporation (NERC) and/or the Electricity Information Sharing and Analysis Center (E-ISAC)

NERC is an entity that is certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk power system but that is not part of the Federal Government. This information would be submitted to help fulfill the respondent's requirements under NERC's reliability standards.

If approval is given to alert NERC and/or E-ISAC the Form will be emailed to systemawareness@nerc.net and/or operations@eisac.com when it is submitted to DOE. DOE is not responsible for ensuring the receipt of these emails by NERC and/or E-ISAC.

☒ Notify NERC | ☒ Notify E-ISAC